Service Function Chaining (SFC): Subscriber and Host Identification Considerations
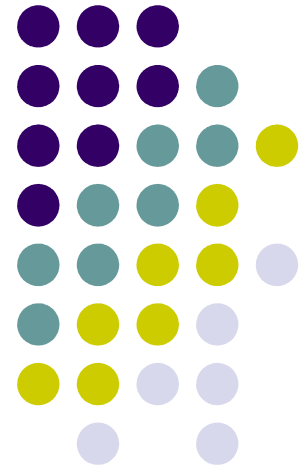
draft-sarikaya-sfc-hostid-serviceheader
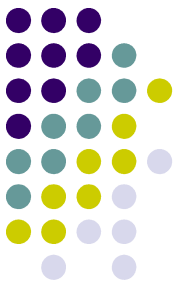
Behcet Sarikaya(sarikaya@ieee.org)

Dirk von Hugo(Dirk.von-Hugo@telekom.de)

Mohamed Boucadair (mohamed.boucadair@orange.com)

*IETF#94, Yokohama, November 2015*

On (Per-subscriber) Policies

- Some service deployments require **enforcing policies based on the internal IP address/prefix**, a subscriber identifier, or a combination thereof.

    – Typically denoted as: Per-subscriber policies

- These policies may be enforced by **one or multiple Service Functions**

- These Service Functions may be **located anywhere within an SFC-enabled domain**

- The exact set of policies to be enforced are **deployment-specific**.
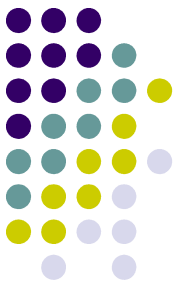
The Problem

- A Service Function that needs to enforce per-subscriber or per-host policies **may not have access** to the internal IP address/prefix or su bscriber Identifier (MAC@, Line ID, etc.)
  - Because of the presence of NATs
  - Difficult to access to a Layer 2 information when the SF is located upstream
- **How to pass that information to upstream SFs for the sake of policy enforcement?**
- Explicit authentication is out of scope

3
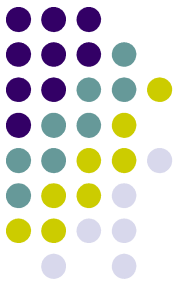
Sample Use Case
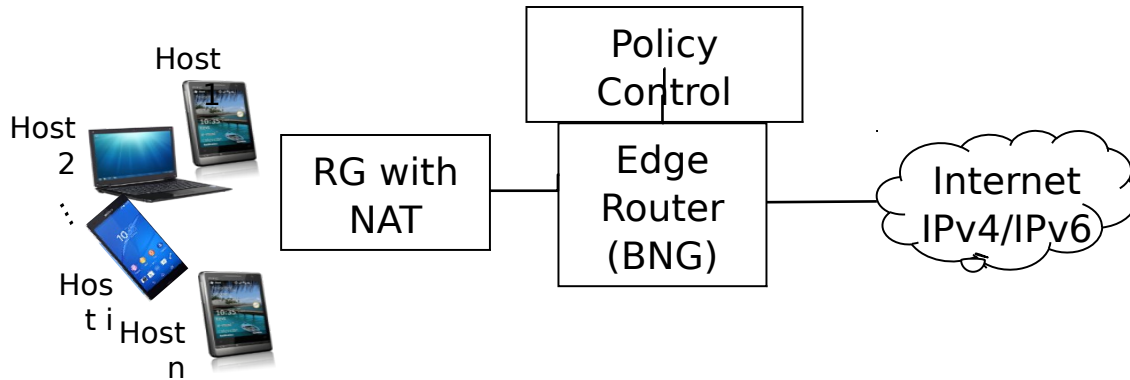
- Scenario: multiple devices with different policies (usage profiles/patterns) owned by same subscriber are behind NAT (e.g. residential home gateway, RG)
    - Smart home sensors
    - Home network (devices) configuration tool
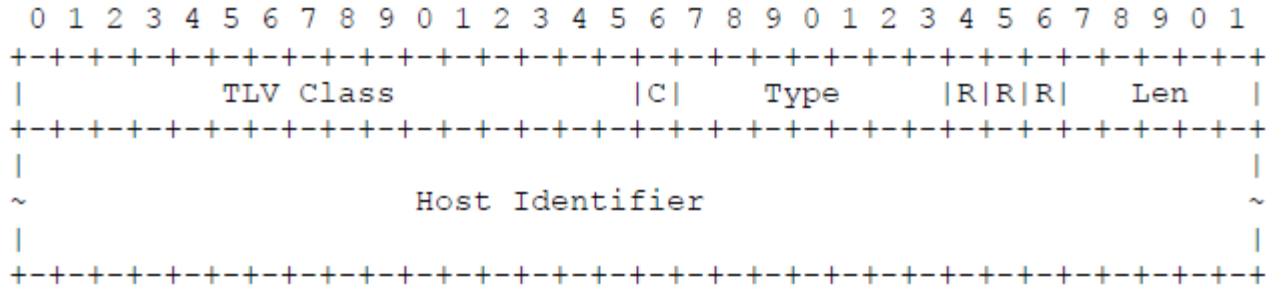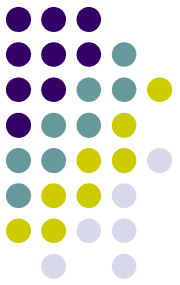   - Parents and kids personal devices
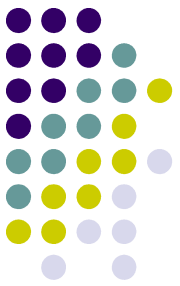
The Solution

- **Pass** the "**identification**" data to be consumed by upstream SFs in a dedicated **NEW** context object
  - As part of the NSH header
  - Compliant with Section 4.9 of RFC 7665 (« Sharing metadata »)

- Two context headers are specified:
  - Host Identifier
  - Subscriber Identifier

- Defined as **Optional Variable Length Metadata**
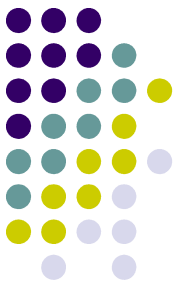
Introducing Host Identifier Metadata

- Host Identifier: Can be IPv4 or IPv6 address, IPv6 prefix, a subset of IP address/prefix, a MAC address, or any deployment-specific identifier. It could also be in Root NAI format containing arbitrary number of characters [TS23.003].

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           TLV Class             |C|    Type    |R|R|R|   Len   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                      Host Identifier                          ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Introducing Subscriber Id Metadata

- Subscriber Identifier: Conveys an opaque subscriber identifier.
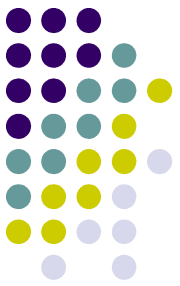 - e.g., International Mobile Subscriber Identity (IMSI) for mobile networks

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          TLV Class            |C|    Type     |R|R|R|   Len   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                     Subscriber Identifier                     ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
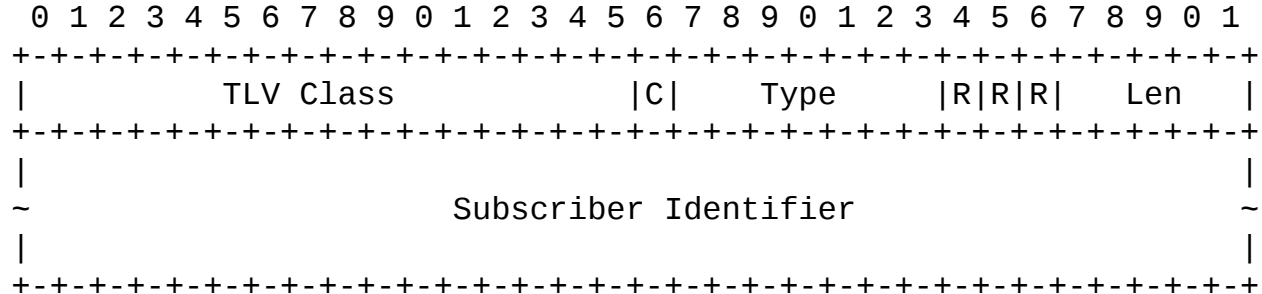
- Two headers are specified to accommodate deployments that require passing both an internal IP address/prefix and a subscriber identifier.

7

Privacy Considerations

- Privacy-related consideration for passing personalized and thus sensitive information have been addressed in the draft, e.g.,
  - Misconfiguring SFC egress nodes is a threat that may have negative impacts on privacy (e.g., some operational networks leak the MSISDN outside).
    - MUST NOT be exposed outside the operator's domain
  - No visible mapping between host ID and subscriber ID
  - CPE MUST NOT leak non-authorized information to the service provider by means of an SFC header.
  - Also tackled by draft-ietf-sfc-control-plane and RFC 6967, RFC7665
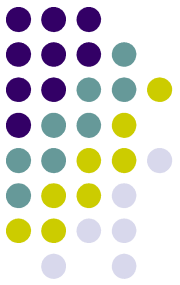
Next steps

- Comments and contributions are welcome
- Any interest from the WG to document such considerations?
- What are the next steps for this effort?
    - Consider adoption as a standalone document?
    - Merge with an existing draft?